YGN ETHICAL HACKER GROUP

Whitepaper

Disclosure Vulnerability: phpinfo.php

By

d0ubl3_h3lix

Sun Jul 16, 2006

Php Developers usually use phpinfo() function in a test file like phpinfo.php or test.php to let them quickly know the php version and its installed features or plug-ins.

It's good but on the other hand, this makes the attacker easily grap your web server information with just a browser. Any other ways the attacker find your phpinfo file? Well, he can use GH (Google Hacking - using Google to find sensitive information) to find it like:

```
intitle: phpinfo () + site: www.yourwebsite.com
```

The phpinfo file shows the valuable information for RECON State of hardcore hacking like:

- System
- Build Date
- Configure Command
- Server API
- Virtual Directory Support
- Configuration File (php.ini) Path
- Apache Version
- Apache API Version
- Server Administrator
- Server Root

And many other. Attackers do not even need to port/services scan. Thus, they can bypass possible IDS detection.

Countermeasures:

Don't put phpinfo file on your server. If you are a server admin, routinely scan sensitive php files to prevent such threat.

Group Contributions:

Added by br0 at Jan 05th, 2008:

We can find that phpinfo.php easily by Google hacking technique.

Type

```
intitle:phpinfo.php “PHP Version”
```

in Google search box and you may see many sites with phpinfo.php on search results.

After that you can test its XSS executable or not by following technique.

```
http://www.yoursite.com/phpinfo.php?a[]=<script>alert(‘XSS Executable’)</script>
```

If you see an alert box pop up that says ‘XSS Executable’, then that version of php info is XSS vulnerable.

Site admins need to remove that phpinfo.php file or change chmod (files and folder attribute).